eSecurity

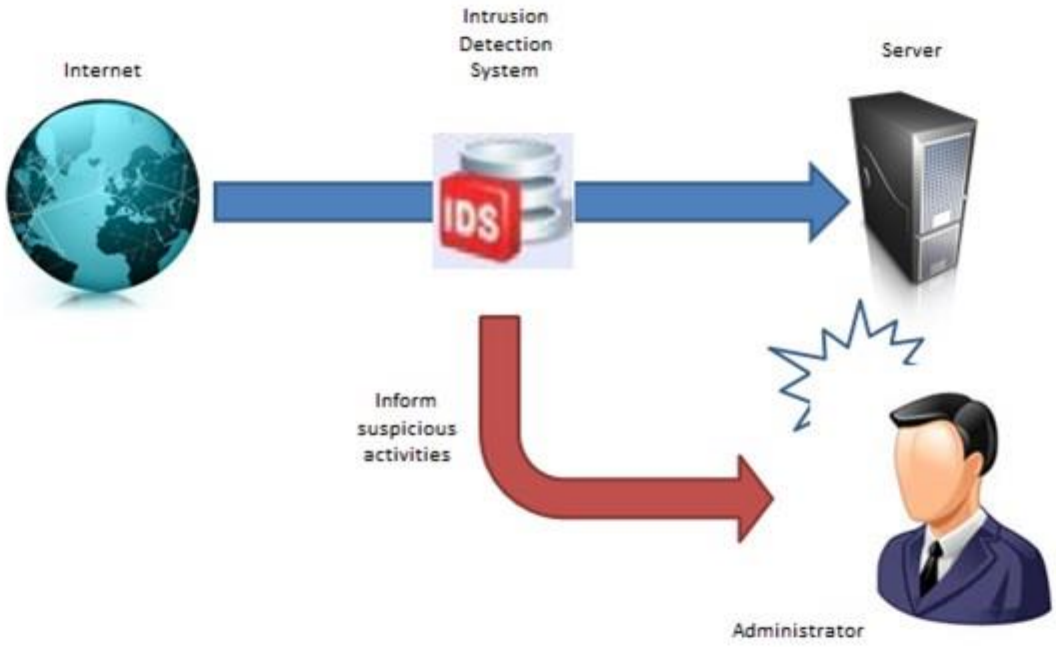
Treinamentos em Segurança da Informação

O que temos para hoje?

Menu do dia:

- ✓ **Sistema de Detecção de Intrusões**
  - ✓ Entendendo IDS
  - ✓ IDS em redes com Switches
  - ✓ Entendendo Port Mirroring ou SPAN
  - ✓ IDS em redes com Switches: Topologia
  - ✓ IDS em redes de alta velocidade
  - ✓ Principais IDSs do mercado: Snort
  - ✓ Principais IDSs do mercado: Suricata
- ✓ **Sistema de Prevenção de Intrusões**
  - ✓ Entendendo IPS
  - ✓ IPS em topologia de rede
  - ✓ IPS em topologia de rede 2
  - ✓ IPS em topologia de internet
  - ✓ Modelos de IPSs comerciais
  - ✓ Modelos de IPSs Livres

Sistema de Detecção de Intrusos



Entendendo IDS

Sistema de detecção de intrusos ou simplesmente IDS (em inglês: Intrusion Detection System) refere-se a meios técnicos de descobrir em uma rede quando está tendo acessos não autorizados que podem indicar a ação de um hacker, ou funcionários mal intencionados.

Com o acentuado crescimento das tecnologias de infraestrutura tanto nos serviços quanto nos protocolos de rede torna-se cada vez mais difícil à implantação de sistema de detecção de intrusos.

Esse fato está intimamente ligado não somente a velocidade com que as tecnologias avançam, mas principalmente com a complexidade dos meios que são utilizados para aumentar a segurança nas transmissões de dados.

IDS em redes com Switches

A implementação de IDSs em redes comutadas (no caso baseadas em switching) permitem a comunicação direta, não compartilhada entre dois dispositivos. Essa característica introduz algumas dificuldades para a implementação de IDSs se comparada as redes com transmissão por difusão.

Como nesse tipo de rede os dados trafegam diretamente para seus destinos (sem a difusão) torna-se preciso, na implantação de IDSs, algumas soluções específicas.

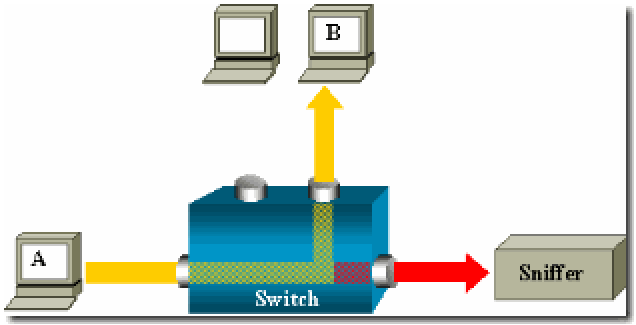
O uso de Port Span consiste na utilização de switches com IDS embutidos. A decisão de sua utilização deve ser discutida antes da compra dos concentradores de rede (switches).

O uso de Port Mirror consiste em fazer no switch o espelhamento do tráfego de uma única porta para outra usada para o monitoramento.

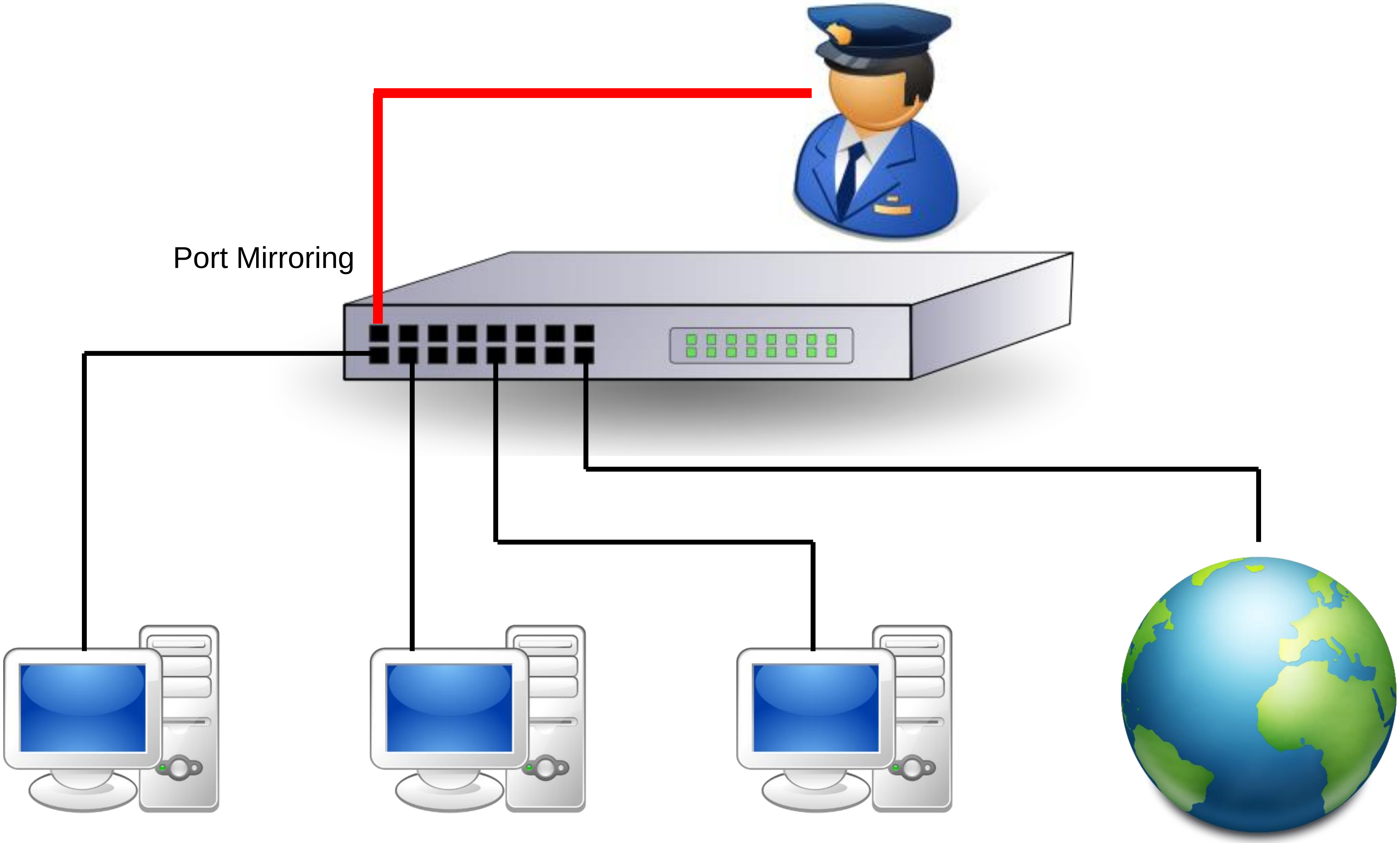
Entendendo Port Mirroring ou SPAN

O SPAN – Switched Port Analyzer, também conhecido como Port Mirroring ou Port Monitoring é a capacidade de espelhar o tráfego de uma porta (ou portas, ou VLAN) para outra.

Entre outras aplicações, esta funcionalidade é muito utilizada em conjunto com equipamentos de análise de rede, que deve receber o tráfego espelhado.



IDS em redes com SWs: Topologia



IDS em redes de alta velocidade

A evolução tecnológica tem também permitido que um maior número de redes possuam altas velocidades de transmissão de dados.

Sob o ponto de vista da implantação de IDS isso se torna um ponto bastante delicado que traz questões importantes na manutenção da infra estrutura de redes, destacando-se:

Os softwares IDS conseguirão analisar toda a grande quantidade de dados que trafegam na rede?

O hardware de monitoramento suportará tamanho tráfego?

Os IDS não irão prejudicar a performance da rede se tornando um gargalo?.

IDS em redes de alta velocidade

Essas, e outras questões, têm sido bastante discutidas, gerando várias soluções para contornar esses problemas ou problemas em potencial.
Destacando-se:

- Aumentar o poder de processamento dos equipamentos
- Monitoração utilizando-se target IDS* definidas pelo administrador
- Direcionamento de tráfego, Toplayer
- Recursos de filtragem dos IDS
- Segregação de IDS por serviço (IDS especialista)

* Target IDS - Monitoração de alguns elementos da rede que são do interesse do administrador (por exemplo, monitoração dos roteadores apenas)

Principais IDSs do mercado: SNORT

Snort é um software livre de detecção de intrusão para rede (NIDS) desenvolvido inicialmente por Martin Roesch, capaz de desenvolver análise de tráfego em tempo real e registro de pacote em redes IP.

Executa análise de protocolo, busca/associa padrões de conteúdo e pode ser usado para detectar uma variedade de ataques, tais como buffer overflows, stealth port scans, ataques CGI, SMB probes, OS fingerprinting, entre outras.

Esta ferramenta é suportada em arquiteturas RISC e CISC e em plataformas das mais diversas, como várias distros Linux (Red Hat, Debian, Slackware, Mandrake, etc.), OpenBSD, FreeBSD, NetBSD, Solaris, SunOS, HP-UX, AIX, IRIX, Tru64, Windows e MacOS X.

Principais IDSs do mercado: Suricata

Suricata é um ID/PS baseado em regras que utiliza essas regras desenvolvidas externamente definidas para monitorar o tráfego de rede e fornecer alertas para o administrador de sistema quando ocorrerem eventos suspeitos .
Projetado para ser compatível com os atuais componentes de segurança de rede, Suricata apresenta funcionalidade de saída unificada e opções bibliotecas conectáveis para aceitar chamadas de outros aplicativos.

A versão atual do Suricata é executada em uma plataforma Linux 2.6+ que suporta configurações de monitoramento de tráfego online e passiva, capaz de lidar com vários níveis de tráfego gigabit.

Sistema de Provenção de Intrusos

Entendendo IPS

Os sistemas de prevenção de intrusões, do inglês ***Intrusion prevention systems (IPS)***, evoluíram no final dos anos 1990 para resolver as ambiguidades no monitoramento de rede passivo, ao colocar a detecção online.

A princípio, o IPS era apenas um sistema de detecção de intrusos (IDS) que possibilitava alguma interação com o firewall para controlar o acesso.

Em pouco tempo foi necessário desenvolver algo mais robusto, pois apenas comandar o firewall não bastava: ainda era possível que ao menos aquele pacote malicioso trafegasse na rede. A solução era implementar formas inteligentes de bloqueio dentro do IPS.

Visto como uma extensão do firewall, o IPS possibilita decisões de acesso baseadas no conteúdo da aplicação - e não apenas no endereço IP ou em portas, como os firewalls tradicionais trabalham. Entretanto, nada impede que, para otimizar a performance, muitos IPS utilizem regras baseadas em portas e endereço IP.

Entendendo IPS

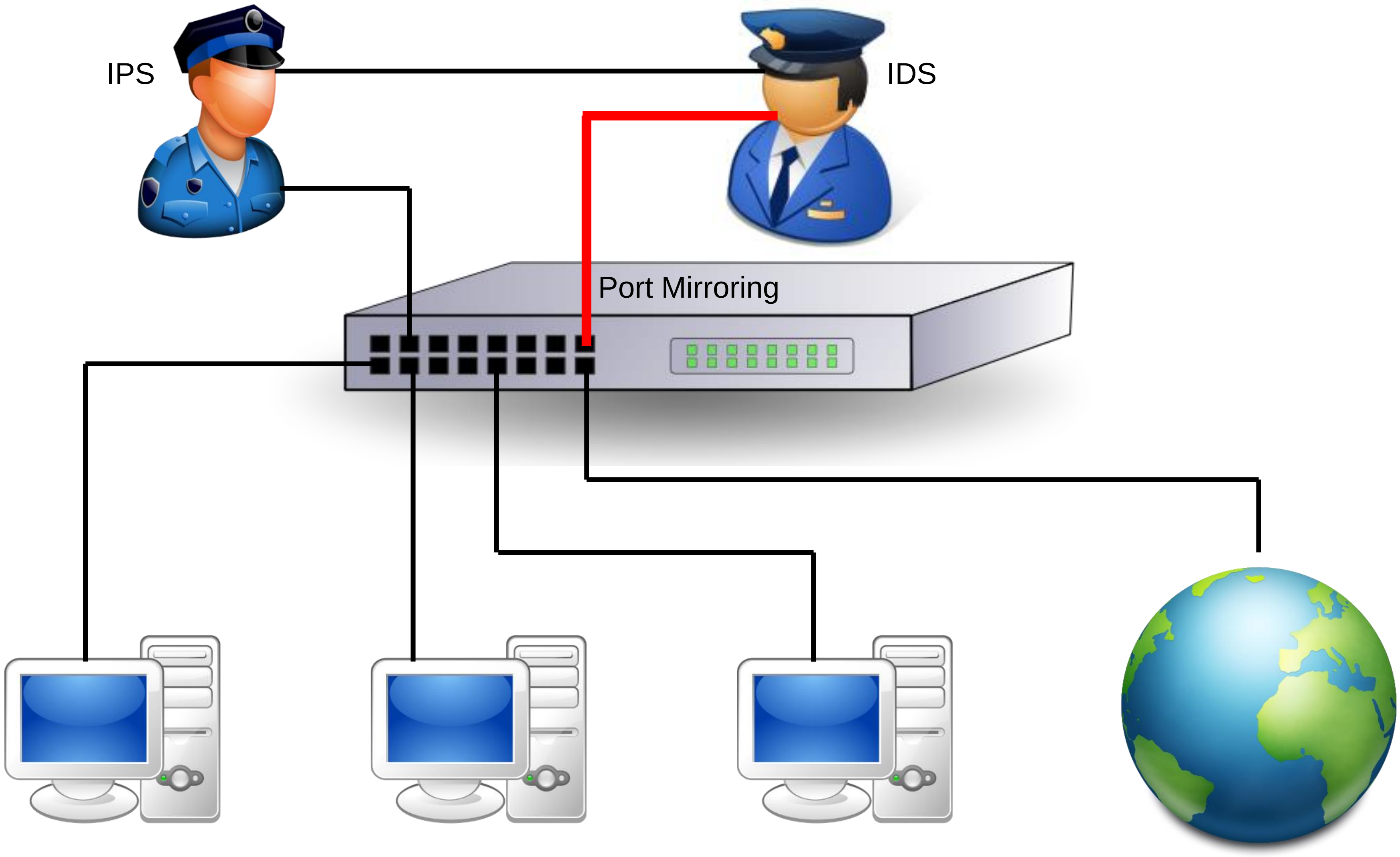
O IPS também pode servir secundariamente como um serviço de nível de host, prevenindo atividades potencialmente maliciosas.

Existem vantagens e desvantagens, tanto no IPS baseado em host como no IPS baseado em rede.

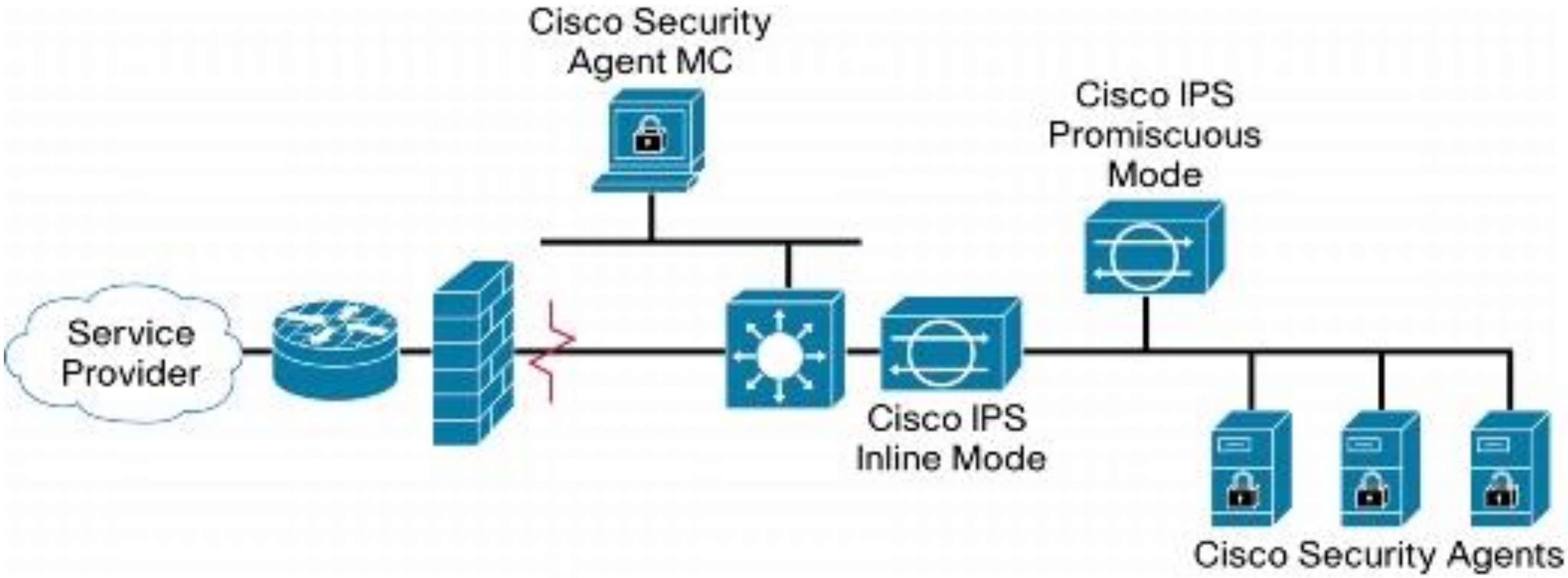
Em alguns casos, as tecnologias podem ser complementares. Porém, não se pode esquecer que grande parte da tecnologia de IPS de rede evoluiu e, hoje, pode tranquilamente exercer também as funções de host.

A vantagem de um sistema de prevenção de intrusos está em ser um excelente detector de tráfego malicioso com uma média de falso positivo e falso negativa baixa.

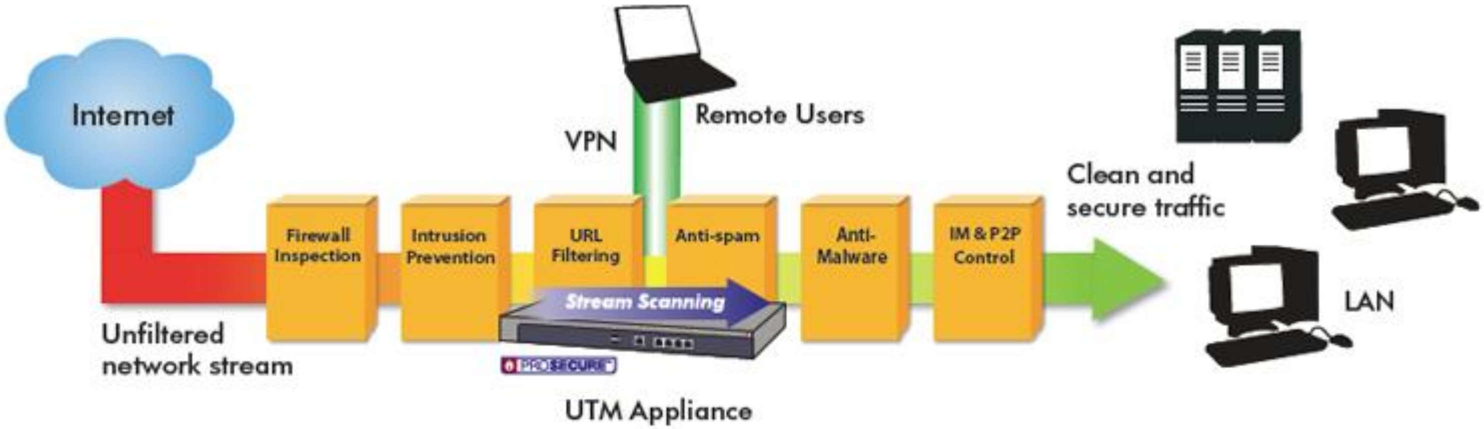
IPS em Topologia de Rede



IPS em Topologia de Rede



IPS em Topologia Internet



Modelos de IPSs Comerciais

Cisco ASA 5500 Series IPS Solution

- Obtém Prevenção de Intrusão, líder de mercado, com firewall, VPN e segurança de conteúdo opcional
- Proteger os pequenos negócios e redes de grandes empresas à beira da Internet, campus e centro de dados
- Reduz os custos operacionais e de implementação, atinge até 10 Gb desempenho inspeção

Modelos de IPSs Comerciais

Enterprise-class IPS

Obtém Prevenção de Intrusão, líder de mercado, com firewall, VPN e segurança de processamento dedicado, isso significa que as principais funções não concorrem para o processamento de ciclos com suas outras funções de segurança, o que acontece em uma única CPU ou ASIC/CPU.

Um formato de assinatura uniforme que elimina processos redundantes, comuns a várias soluções de mecanismo de verificação (remontagem TCP, pesquisa política, fiscalização, etc).

Software passagem única, ao qual significa que o seu tráfego é verificado apenas uma vez, não importa quantos elementos políticos estão em uso.

Modelos de IPSs livres

Suricata

- O Suricata ID/IPS pode ser instalado nos sistemas operacionais Linux, FreeBSD, OPENBSD, Mac OS X e Windows
- Carregamento de grandes quantidades de máquina baseada em dados de reputação
- Regras de Reputação utilizando a chave “iPrep”

*iPrep é uma ferramenta que permite preparar e manipular os arquivos de firmware

Chega por hoje

www.eSecurity.com.br

E-mail: alan.sanches@esecurity.com.br

Twitter: @esecuritybr e @desafiohacker

Skype: desafiohacker

Fanpage: www.facebook.com/academiahacker